AO 106 (Rev. 04/10) Application for a Search Warrant (USAO CDCA Rev. 01/2013)

ORIGINAL

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
3261 Grand Avenue
Huntington Park, California 90255

Case No. M 16 00166

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

FILED
CLERK, U.S. DISTRICT COURT
JAN 25 2016
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sections 2252A(a)(2) (Receipt and distribution of Child Pornography), 2252A(a)(5)(B) (Possession of child pornography), and 2251(d)(Advertisement of child pornography)]	See attached Affidavit

The application is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

LODGED
2016 JAN 25 PM 1:1
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES
BY:

Applicant's signature

Rajiv Patel, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/25/16

Judge's signature

City and state: Los Angeles, California

Suzanne H. Segal, U.S. Magistrate Judge
Printed name and title

AUSA: Karen I. Meyer KIM

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be searched is described in Attachment A and as follows: The property is located at 3261 Grand Avenue, Huntington Park, California 90255, (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a single-family residence that is white-stucco in color. It has an iron/concrete fence surrounding the front of the residence. There is a large bay window to the right of the front door. The house has a red tile roof. The number "3261" is written on the curb directly in front of the SUBJECT PREMISES.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(d) (advertisement of child pornography), specifically:

a. Child pornography, as defined in Title 18, United States Code, Section 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in Title 18, United States Code, Section 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in Title 18, United States Code, Section 2256.

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

e. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to P2P file sharing software.

g. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider.

h. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of 3261 Grand Ave., Huntington Park, California 90255 (the "SUBJECT PREMISES").

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of any digital device(s) found inside the SUBJECT PREMISES.

j. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

k. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The team searching the digital data also may use sophisticated tools, such as forensic hashing tools, to identify child pornography (including, but not limited to, "Encase" and "Forensic Tool Kit," or "FTK"). Forensic hashing is the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data (such as a particular file). If the data is changed, even very slightly (such as the addition or deletion of a comma or a period), the identifier should change. A hash value can be thought of as a "digital fingerprint" for data. The team searching digital devices in this case will also use a "hash set," which contains the hash values of image and video files associated with known identified victims of child pornography to determine whether these files are stored within a digital devices. Because this "hash set" is constantly being updated as investigations result in the rescue of children depicted in child pornography images/videos, it will not contain the hash values of all currently identified image and video files. The team searching the digital devices

will only use search protocols specifically selected to identify items to be seized under this warrant.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest),

only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Rajiv Patel, being duly sworn, do hereby depose and state:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed for approximately eleven years. During my tenure as a Special Agent, I have conducted and participated in numerous investigations of criminal activity. During the investigation of these cases, I have executed and participated in the execution of approximately two hundred search and arrest warrants and seized evidence of violations of United States law. I have completed more than 48 hours of instruction on how computers and the Internet are used by individuals to sexually exploit children. I have conducted numerous investigations of people who have demonstrated a sexual interest in children, both domestically and abroad. In 2013, I spent two months in the Kingdom of Cambodia investigating and preparing for prosecution cases against American citizens who had traveled to Cambodia for the purpose of engaging in sex with minors there. I attend several yearly trainings and conferences related to child exploitation investigations and have done so for the past ten years. I have been trained and certified to conduct child victim forensic interviews and have performed several of these interviews. I currently investigate the sexual exploitation of children and child pornography in the Central District of California as part of the Southern California Regional Sexual Assault Felony Enforcement (SAFE) Team. The SAFE Team is responsible for enforcing federal criminal statutes involving the sexual exploitation of children under Title 18, United States Code, Section 2251, et seq.

2. Through my training and experience, I have become familiar with the methods of operation used by people who are involved with offenses involving the sexual exploitation of

children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses. My experience in investigations in this regard has supplemented my understanding of how people involved in offenses relating to the sexual exploitation of children use the Internet to further those offenses.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a warrant to search the premises located at 3261 Grand Avenue, Huntington Park, California 90255, the "SUBJECT PREMISES," more fully described below and in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(d) (advertisement of child pornography).

4. The facts set forth in this affidavit are based upon my personal observations and training and, where noted, information related to me by other law enforcement officials and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

III. PREMISES TO BE SEARCHED

5. The premises to be searched is described in Attachment A and as follows: The property is located at 3261 Grand Avenue, Huntington Park, California 90255, (the "SUBJECT PREMISES"). The SUBJECT PREMISES is a single-family residence that is white-stucco in color. It has an iron/concrete fence surrounding the front of the residence. There is a large bay

window to the right of the front door. The house has a red tile roof. The number "3261" is written on the curb directly in front of the SUBJECT PREMISES.

IV. SUMMARY OF INVESTIGATION

6. Along with other members of law enforcement, I have been investigating individuals who are trading child pornography on the Internet through an instant messaging software application. As set forth in greater detail below, on January 1, 2016, a law enforcement officer acting in an online undercover capacity (the "UC") observed and captured a user of an Internet-based messaging application send CP images to other users, including the UC. The IP address of the computer offering the child pornography relates to the SUBJECT PREMISES through subscriber information and Lexis/Nexis. Thus, I respectfully submit that there is probable cause to believe that the SUBJECT PREMISES contains evidence of criminal activity in violation of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(d) (advertisement of child pornography).

V. DEFINITION OF TERMS

7. The following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "computer" is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

c. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with

roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. The term "Internet Protocol" ("IP") is defined as the primary protocol upon which the Internet is based. IP allows a packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

e. The term "IP Address" is defined as a unique number assigned to each computer directly connected to the Internet (for example, 172.191.142.150). Each computer connected to the Internet is assigned a unique IP address while it is connected. The IP address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP address is only assigned for the duration of that online session.

f. The term "Internet Service Provider" ("ISP") is defined as a business that allows a user to dial into or link through its computers thereby allowing the user to connect to the Internet for a fee. ISPs generally provide only an Internet connection, an electronic mail address, and maybe Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

g. The term "peer-to-peer" ("P2P") has come to describe applications or programs that allow users to exchange files with each other directly or through a mediating

server, via the Internet.[1] A decentralized peer-to-peer file transfer network does not follow a model using different clients or servers; but, rather, it is a network of equal peer computers that simultaneously function as both "clients" and "servers" to the other users on the same network.

h. The term "open source" is defined as software that includes a free license; in other words, it is freely available to everyone using the Internet.

i. The term "share folder," in the context of P2P software, is a folder or directory on a computer's hard drive, which a P2P user can set up to share his/her contents with other computers on a peer-to-peer network.

j. The term "browsing" is used in reference to peer-to-peer networks, refers to the ability of a P2P user to look at or browse the shared files of another P2P user.

k. The terms "jpeg," "jpg," "gif," "bmp," and "art" are defined as graphic image files, namely, pictures.

l. The terms "mpeg," "mpg," "mov," "avi," "rm," and "wmv" are defined as video or movie files. To use these video files, one needs a personal computer or other digital devices with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

m. The term "Mobile instant messaging ("MIM")" is a messaging service that uses instant messaging ("IM") via mobile devices, employing various technologies such as text messaging, Wireless Access Protocol ("WAP") and General Packet Radio Service ("GPRS").

---

[1] A computer that is performing tasks for other computers that are connected to it is often called a "server." A "client" computer is one that is connected to a server and is making requests of the server.

Unlike SMS, MIM notifies the user when those in the contacts list are available or not available for chat.

n. The term "smart phone" or "mobile device" is a cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system, Web browsing and the ability to run software applications. In addition, a mobile device is a small computing device, typically small enough to be handheld (and hence also commonly known as a handheld computer or simply handheld) having a display screen with touch input and/or a miniature keyboard.

o. The term "app" is a self-contained program or piece of software designed to fulfill a particular purpose; an application, especially as downloaded by a user to a mobile device or smart phone.

p. The term "wi-fi" is a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

q. The term "text message" is an electronic communication sent and received by cellular phone, smart phone, and/or mobile device.

r. The term "social network" is a dedicated website or other application that enables users to communicate with each other by posting information, comments, messages, images, etc.

VI. BACKGROUND ON USE OF COMPUTERS, CHILD PORNOGRAPHY, AND PEER-TO-PEER FILE SHARING TECHNOLOGY

8. Based upon my training and experience in the investigation of child pornography and with instant messaging applications ("apps"), and information related to me by other law

enforcement officers involved in the investigation of child pornography generally, I know the following information about the use of smart phones/mobile devices with child pornography:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can scan these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. A growing phenomenon in mobile devices and smart phones is the use of "apps" to communicate between users. One such "app" is called "Kik." "Kik" is a smart phone/mobile device software application that allows people to use Wi-Fi to send text messages. It is a cross platform app, which means one can use Kik for either PC or Mac and can even use Kik for communication between devices. As more people are using their smart phones and mobile devices as their primary internet device, applications like Kik are being used more frequently.

c. Kik allows users to send many text messages. In addition, Kik allows users to send photographs, videos, and other digital data. Kik is built to look and act like texting with users. Kik asks the user to create a username to chat with people they know, known as "friends". Kik can send out invitations to "friends" by text message, email, or through social networks.

d. On many occasions, individuals who have a sexual interest in children use smart phones and mobile devices to communicate with other individuals of similar interest, or prey on under age children, using mobile device applications. Individuals with a sexual interest

in children become acquainted with like-minded people, or minors, through the Internet and then exchange phone numbers, email addresses, and other methods of communications, such as Kik accounts.

VII. STATEMENT OF PROBABLE CAUSE

A. Online Investigation by Special Agent Rajiv Patel

9. On or about January 20, 2016, I spoke with a FBI Task Force Officer ("TFO") Randall Snyder over the telephone and obtained his reports and learned the following:

10. On January 1, 2016, TFO Snyder was conducting proactive investigations into the online trading of child pornography on the "Kik" messenger application when a suspect was observed in the "baby" online chat room. The suspect was identified with the user name "babyandtoddlers" and a screen name of "B Bbb" and asked to "trade babies." The screen name and username are specific identifiers of the suspect. Furthermore, "B Bbb" has an associated graphic-icon, which is picture of a folded diaper with the "Elmo" Sesame Street children's character on the diaper. On January 1, 2016, from approximately 4:54 a.m. through 5:13 a.m. (Arizona time) "babyandtoddlers" proceeded to trade images and videos of child pornography with other individuals in the "baby" chat room, including with the UC. The following is an example of the images that were sent by "babyandtoddlers" to the members of the "baby" online chat room:

a. One image is of a very young nude boy, approximately five years old, based on my training and experience, who appears to be performing oral sex on an adult male.

b. Another image shows a female, appearing to be an infant, based on my training and experience, lying on her back with her vagina exposed. An adult male has his exposed penis over the child's vagina and appears to be ejaculating on the baby.

c. A third image is a close up of a nude girl's mid-section, approximately one or two years old, based on my training and experience. The girl is being vaginally penetrated by an adult male's penis.

11. The suspect also sent additional images and videos similar to the described images above. TFO Snyder captured these exchanges of images, videos, and text messages.

12. The suspect also asked if anyone had any links to good groups and wanted to trade videos. The suspect advised one user "I love babies." The user's transactions were screen captured and the images and videos that were able to be downloaded were preserved.

B. Identification of Subscriber of SUSPECT IP ADDRESS

13. On January 7, 2016, a subpoena was sent to Kik to try and identify the Kik user associated with Kik username "babyandtoddlers" and the associated Kik screen name of "B Bbb" for the last six months. On January 11, 2016, Kik returned information related to the subpoena. Kik identified the account holder's email address as samsungboy1122334455@gmail.com. This email address was unconfirmed and online searches did not locate any accounts attached to that email. An IP address of 68.190.213.170 (the "SUSPECT IP address") was the static IP provided by Kik for the period covering December 14, 2015, through January 10, 2016. In addition, the SUSECT IP address belonged to the Internet service provider, Charter Communications.

14. A subpoena was obtained and provided to Charter Communications for the SUSPECT IP address on January 12, 2016, for subscriber and service information during the time period where the SUSPECT IP address distributed the images of child pornography. A return from Charter was obtained on January 20, 2016, which indicated the SUSPECT IP address was assigned to Manuel Garcia, at 3261 Grand Avenue, in Huntington Park, California (the

SUBJECT PREMISES) from December 20, 2015, through January 14, 2016, which is the timeframe the suspect had distributed the images of child pornography.

15. On January 20, 2016, I conducted a check in the LexisNexis records database for the name "Manuel Garcia." The LexisNexis database is a collection of publicly available information. In the LexisNexis database, the address listed for "Manuel Garcia" is "3261 Grand Ave., in Huntington Park, California 90255." Furthermore, Lexis/Nexis revealed an additional resident named Richard Garcia. According to Lexis/Nexis, Richard Garcia is a registered sex offender. The registration offense is listed as "possess or control obscene matter depicting a minor."

16. Based on the information above, I respectfully submit that there is probable cause to believe that someone at the SUBJECT PREMISES possessed, and made available for distribution, multiple files containing child pornography using the SUSPECT IP ADDRESS.

VIII. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH SEXUAL INTEREST IN CHILDREN

17. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive

poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material – that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc. – in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and/or videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy

correspondence from other child pornography distributors/ collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

18. Even if Manuel Garcia or Richard Garcia—or another person with access to the SUSPECT IP ADDRESS at the SUBJECT PREMISES—used this or another computer located elsewhere to access the Internet and illegal child pornography, it is likely that evidence of this access will be found in the SUBJECT PREMISES. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, and/or stored on iPods, Blackberries, or cellular telephones. Because someone at the SUBJECT PREMISES likely collects and values child pornography, which is easily-stored and duplicated, there is probable cause to believe that evidence of a child pornography collection will be found in the SUBJECT PREMISES.

IX. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop,

laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled

environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains

a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime,

indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

20. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

X. ITEMS TO BE SEIZED

21. Based on the foregoing, I respectfully submit that there is probable cause to believe that the items to be seized, listed in Attachment B, constitute evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(d)(advertisement of child pornography).

XI. CONCLUSION

22. For all the reasons described above, there is probable cause to believe that the evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and

distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(d) (advertisement of child pornography), as described in Attachment B to this affidavit, will be found in a search of the SUBJECT PREMISES, which is further described above and in Attachment A of this affidavit.

RAJIV PATEL, SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

SUBSCRIBED TO AND SWORN BEFORE ME
THIS 25 DAY OF JANUARY 25, 2016

THE HON SUZANNE H. SEGAL
UNITED STATES MAGISTRATE JUDGE